CenturyLink Technology Solutions

CenturyLink Technology Solutions Service Guide

Threat Management Service 1.0

This CenturyLink Service Guide ("SG") sets forth a description of Threat Management Service ("Service") offerings by CenturyLink, including technical details and additional requirements, if any. This SG is subject to and incorporated into the Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order. For avoidance of doubt, any references in the Agreement, Schedules, or Service Orders to SSG, shall mean SG

Version	Previous	Section Modified	Date
SEC-20141111-SG-ThreatManagementService	SEC-20140922-SG-ThreatManagementService	ALL	November 11, 2014

CenturyLink Technology Solutions
www.centurylink.com/technology

Town & Country, MO 63017
Office: 314.628.7000

Table of Contents

Service Description

1. **Service Description:** Threat Management is a CenturyLink provided service (the "Service") that combines internal vulnerability scanning of Customer servers with correlation of real-time events detected by CenturyLink-managed Network Intrusion Detection Service (NIDS) or Managed Firewall Service 3.0 with IPS ("Related Security Services"). The Customer chooses whether the Service is CenturyLink Managed, in a CenturyLink Hosting Environment (Colocation), or on Customer Premise (definitions of each option are located in Definitions. The Service is only available to Customers that also purchase the CenturyLink Related Security Services under separate terms and charges. The standard features of the Service consist of installation, configuration, administration, monitoring, maintenance and support of a CenturyLink-provided Vulnerability-Scanning Appliance (CenturyLink Equipment) for the components listed in section 1.1. The Service Level Agreement (SLA) associated with this service guide can be found in Appendix A.

    1.1. **Service Components:**
        1.1.1. **All Environments:**
            1.1.1.1. **Appliance:** CenturyLink provides a dedicated appliance with each instance of the Service. The number of scanning appliances required is dependent upon the number of devices to be scanned, the Customer's network architecture, and the Customer's security policy. Each instance of the Service will include the ability to scan a block of 10 IP addresses.
        1.1.2. **CenturyLink Managed Only:**
            1.1.2.1. **VLAN:** Installation of the Service within a CenturyLink Managed environment will include (1) VLAN, (1) 10/100/1000 connection to the CenturyLink Equipment.

    1.2. **Installation:** CenturyLink will provide the installation tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities
        1.2.1. **Setup:** CenturyLink will perform set-up and implementation based on the Service profile provided by Customer

    1.3. **Configuration:** CenturyLink will provide the configuration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.
        1.3.1. **Test Period**: Once the Customer has provided all required information requested during the Threat Management Service set-up consultation, CenturyLink will install and configure the CenturyLink Equipment, enable and test the threat-event correlation system for a period of one full week. This will allow CenturyLink security engineers to evaluate the correlated alert traffic for false alarms and make appropriate modifications, if required.
        1.3.2. **Go Live**: After the test period and upon written approval from Customer, the Service will be considered fully operational ("live").
        1.3.3. **Updates**: CenturyLink system administrators will perform up to three service modifications and configuration changes per month, as requested by the Customer. Additional change requests (in a given month) may incur additional fees. Configuration changes may include changes to frequency of vulnerability scans and changes to vulnerability scanning targets.

    1.4. **Administration:** CenturyLink will provide the administration tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.
        1.4.1. **System Administration:** CenturyLink will manage all system administration passwords for Threat Management Service. Customer will not have access to Threat Management system passwords or be able to make direct changes to the system configurations. Customer must instead submit change requests to CenturyLink to make configuration changes.

1.5. **Monitoring:** CenturyLink will provide the monitoring tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.5.1. **Monitors:** Scan results of Customer's devices are reported via CenturyLink's secure Web-based portal.

1.5.2. **Correlation:** Correlation of identified critical vulnerabilities and threats that are deemed critical ("critical threats") for selected devices are prioritized as "Critical Alerts," and responded to by CenturyLink's Security Operations Center (SOC) and reported via the CenturyLink's Security Services portal.

1.5.3. **Alerting:** Alerting of correlated critical threats with critical vulnerabilities is initiated by CenturyLink's security personnel in accordance with the methods in Table 6.0 Response Times.

1.5.3.1. The CenturyLink Service Center receives and reviews critical alerts that have been correlated by the Service, based on vulnerability scan data and events issued by the CenturyLink Related Security Services. Related Security Services generate alerts upon encountering network traffic patterns that may indicate suspicious activity.

1.5.4. **Scanning:** Scanning duration is determined by the number of IP addresses scanned and the level of scan performed.

1.5.5. **Notifications:** CenturyLink's notification for this Service is defined in Table 6.0 Response Times.

1.5.6. **Threat Management Review:** Two times per year upon Customer request, CenturyLink provide a review of the Customer's installation. Each review (up to 8 hours per review) may be conducted telephonically. To initiate a bi-annual review. Customer should contact the CenturyLink Service Center to open a ticket.

1.6. **Maintenance and Support:** CenturyLink will provide the maintenance and support tasks marked with an "X" in the CenturyLink column in Table 1.0 Roles and Responsibilities.

1.6.1. **Upgrades:** CenturyLink may periodically upgrade the security software to maintain the latest versions in operation. If CenturyLink determines an upgrade is necessary, CenturyLink will work with Customer to schedule a time to make necessary changes, preferably during the Scheduled Maintenance Windows. Customer must allow CenturyLink to make these changes within five (5) business days of receipt of the request from CenturyLink, or CenturyLink's obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes. If CenturyLink determines that an emergency security change is required, CenturyLink will make the change as quickly as possible. CenturyLink will make commercially reasonable attempts to contact the Customer's technical contact prior to making said change.

1.6.2. **Hardware Repair:** If required, CenturyLink will be responsible for repairing and/or replacing hardware provided by CenturyLink with the Service, except where such repair or replacement is due to any act or omission by Customer or its agents, in which case, Customer may be invoiced for the repair or replacement cost of the appliance.

2. **Customer Responsibilities:** Customer is responsible for all tasks marked with an "X" in the Customer column in Table 1.0 Roles and Responsibilities. Customer acknowledges and agrees that its failure to perform its obligations set forth in Table 1.0 may result in CenturyLink's inability to perform the Services and CenturyLink shall not be liable for any failure to perform in the event of Customer's failure.

2.1. **Physical Site Requirements**

2.1.1. **Network Topology:** Customer must provide CenturyLink with a topology of their existing network prior to any security review, installation of the CenturyLink Equipment, and commencement of the Service. Customer must notify CenturyLink in advance of any network topology or system changes that may affect Service. Failure to notify CenturyLink of system changes may result in the inability to monitor and correlate traffic, or the generation of false positives. CenturyLink will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are

not resolved satisfactorily, CenturyLink may modify the Service configuration to reduce repetitive alarms caused by Customer actions that are not indicative of security incidents.

2.1.2. **IP Addresses:** Customer must provide IP addresses for all systems that the CenturyLink equipment is to scan for vulnerabilities.

2.2. **Testing:** Customer shall not attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service or any devices used to deliver CenturyLink services. Without limiting the foregoing, Customer is specifically prohibited from conducting unannounced or unscheduled test firewall attacks, penetration testing or external network scans on CenturyLink's network without the prior written consent of CenturyLink.

2.3. **Rotation of IP addresses:** The scanned IP addresses will correspond to the subnets provisioned for the Customer managed hosting environment during the initial configuration. Once the LAN is built, subnet and IP addresses will not be rotated within the first 12 months, unless approved by CenturyLink.

2.4. **Access Control Lists:** Remove any Access Control List that interferes with management connections; the Customer must allow CenturyLink access for management and monitoring.

2.5. **Equipment Access:** Give CenturyLink and others working for CenturyLink access to CenturyLink Equipment as follows: immediately if there is a service outage and at reasonable times in all other situations. Customer will allow CenturyLink personnel to access the CenturyLink Equipment, where CenturyLink determines such access is necessary to deliver the Service or respond to a security incident.

2.6. **Customer Premise Only:**

2.6.1. **Connectivity:** Provide an always-on connection to the public Internet. Dial-up connection is not sufficient.

3. **Additional Services**: At Customer's option and expense Customer can choose to have CenturyLink complete one or more of the tasks in Table 1.0 with an "X" in the Customer column and/or the services listed below. The items can be added to the standard Service (described in Section 1.0) for an additional fee described in a separate Statement of Work ("SOW") or Service Order. Contact a sales representative for additional information.

3.1. **Expansion Packs:** Expansion Packs are available in blocks of 10 that enable CenturyLink equipment to scan additional IP addresses and are available for separate purchase. Individual Expansion Packs must be associated with one Vulnerability Scanning Appliance, and cannot be divided between multiple Appliances, (i.e., multiple instances of the Service).

3.2. **Additional Ports and VLANs:** For CenturyLink Managed Hosting environments any Port or VLAN requested by Customer after the initial installation of the Service shall be subject to additional, incremental charges.

Tables and Appendices

Table 1.0 Roles and Responsibilities

Activity	Task	CenturyLink	Customer
Installation	Perform set-up and implementation based on the requirements provided by Customer	X	
	Provide all required information requested during the Service set-up consultation		X
	Install and configure the CenturyLink Equipment	X	
	Enable and test the threat-event correlation system for a period of one full week to allow CenturyLink engineers to evaluate the correlated alert traffic for false alarms and make appropriate modifications	X	
	Communicate vulnerability scan data and/or correlated alert traffic		X
	Make required adjustments to threat-management devices and declare Service fully operational	X	
Configuration	Perform an initial threat-management set-up consultation with the Customer	X	
	Identify servers to be included as part of the Service		X
	Determine the number of Vulnerability-Scanning Appliances required	X	
	Provide applicable Customer's network architecture, and the Customer's security policy.		X
	Review Customer's architecture to confirm servers scanned are located on the same logical networks as CenturyLink-managed NIDS and Managed Firewall Service 3.0 with IPS devices	X	
	Determine vulnerability scanning frequency timeframes		X
	Establish alert policy and determine the appropriate response procedure		X
	Answer Customer's questions regarding the Service	X	
Administration	CenturyLink system administrators perform up to three service modifications and	X	

Activity	Task	CenturyLink	Customer
	configuration changes per month as requested by Customer		
	Investigate alerts Related Security Services alerts that are correlated with discovered vulnerabilities	X	
Monitoring	Request CenturyLink review of Threat Management Service		X
	Provide a review (up to twice a year) of Customer Threat Management Service	X	
	Provide access to Service alert reports for the previous 90 days via a secure Web-based portal	X	
	Implement various health checks such as ICMP (e.g., ping) monitoring of the CenturyLink Equipment to determine system availability	X	
Maintenance and Support	Notify Customer via phone or email to initiate corrective action in the event that the vulnerability scanner fails to respond	X	
	Request changes by contacting the CenturyLink Response Center		X
	24/7 support for Service problem resolution and Customer inquiries are included	X	
	Ensure that all Customer permissions of any kind needed for the delivery of the Service are in place at all times		X

Table 2.0 Customer Installation Requirements – Customer Site in IDC (Colocation site) and Customer Premise

Item	Requirement
Physical Environment	Predefined and adequate rack shelf or tabletop space for installation, with unobstructed entry for CenturyLink and others working for CenturyLink. CenturyLink will provide specifications at the initial kickoff.
Electrical Power	Electrical outlet.
	Extension wiring if distance to the electrical outlet is greater than 6 feet.
	Power supply ready at installation location.
Support modem communication	Dedicated analog (dial-up) line for the support modem with inbound direct dial capability.

Item	Requirement
	Extension wiring if distance to the analog line termination is greater than 6 feet.
LAN Connectivity	Extension wiring if the distance to the LAN connection is greater than 6 feet.
	10/100/1000 network connection into the Customer switching infrastructure.

Appendix A Service Level Agreement

Table 3.0 Response Times

Response Event	Response Time and Procedure
Critical Alarm	CenturyLink personnel will review critical alerts within 15 minutes and will attempt to notify the Customer within 60 minutes, by telephone, pager or electronic mail, as specified in the Customer's escalation procedure. Maps to SLO P1 (Urgent). Reference Service desk SLO link Savvisstation.com, Incident Management section.
Service Configuration and Policy Change Request	CenturyLink will respond to routine configuration and policy change requests within 24 business hours. Maps to SLO P2 (High). Reference Service desk SLO link Savvisstation.com, Request Management section.
Hardware fault resolution time to Service outage	If CenturyLink determines that CenturyLink Equipment must be swapped, CenturyLink will complete the swap by the next business day from the date of problem detection. Installation is performed by party defined in Table 2.0 Installation Details.
IR Consulting	CenturyLink will respond to a request for IR Consulting within 30 minutes.

Response Times SLA

In the event that CenturyLink is unable to provide service within the "Response Time" windows outlined above, the Customer's sole and exclusive remedy shall be a service credit in the amount of three percent (3%) of the affected service MRC for each response time failure. In no event will the credits accrued in any single month exceed, in the aggregate across all response time goals and incidents, thirty percent (30%) of the invoice amount for the affected service.

CenturyLink's obligation to meet stated Response Times will not apply to:

- any problems caused by or associated with the Customer's failure to meet specified Customer Requirements
- underlying Internet access service
- any security tests.

SLA Process

Customer must request any credit due hereunder within 30 days of the conclusion of the month in which it accrues. Customer waives any right to credits not requested within this 30-day period. Credits will be issued once

validated by CenturyLink and applied toward the invoice which Customer receives no later than two months following Customer's credit request. All performance calculations and applicable service credits are based on CenturyLink records and data.

The applicable SLA provides Customer's sole and exclusive remedies for any Service interruptions, deficiencies, or failures of any kind. The SLA and any remedies hereunder will not apply and Customer will not be entitled to receive a credit in the case of an Excluded Event. "Excluded Event" means any event that adversely impacts the Service that is caused by,

a) the acts or omissions of Customer, its employees, customers, contractors or agents
b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink
c) Force Majeure events
d) scheduled maintenance
e) any suspension of Service pursuant to the Agreement
f) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information

General Service Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with the Service, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

Customer shall:

a) Provide CenturyLink with sufficient system passwords, privileges and access to allow CenturyLink to install, configure, monitor and modify the Service.
b) Not attempt (nor instruct or allow others to attempt) any testing, assessment, circumvention or other evaluation or interference with any Service without the prior written consent of CenturyLink.
c) notify CenturyLink at least 5 business days in advance of any changes that may affect the applicable Service (e.g., infrastructure, network topology changes)
d) purchase and maintain a reliable, stable and always-on, high speed connection to the public Internet (i.e., DSL, T1, cable modem etc. -- a dial-up connection is not sufficient) and/or a standard (POTS) telephone line (with direct inward dialling) for each Customer Site to enable CenturyLink to perform remote network management functions.
e) Designate and maintain a Customer Contact during the Service Term (including current contact information). "Customer Contact" means an English-speaking technical point of contact available 24 x 7 with sufficient knowledge, authority and access to address configuration issues, event notifications, system or infrastructure modifications and authentication of applicable CenturyLink systems.
f) For CenturyLink Managed Hosting environments any Ports and VLANs in addition to those included in the standard CenturyLink design shall be subject to incremental charges as set forth in the relevant Order Form. Any Port or VLAN requested by Customer after the initial installation of the Service shall also be subject to additional, incremental charges. Provision of the Service is subject to Customer's compliance with this Section.

CenturyLink may manage all system administration passwords, including root level access, and may do so exclusively. In such case, Customer will not have access to system passwords nor able to make changes to the system configurations and must instead submit change requests to CenturyLink.

CenturyLink may require access to Customer's staging environment that matches production configuration in order to test configuration stability prior to implementing software changes. A successful test on the staging system does not guarantee success on the production system. The Services do not include the development of a comprehensive

change control process. There may be incompatibilities between a Service and particular Customer environments which cannot be resolved. In such cases, CenturyLink reserves the right to withdraw the Service from those particular environments, but only to the extent necessary to resolve the incompatibility and without modifying either party's obligations with regard to unaffected environments.

Customer may incur additional charges if:

a) Customer impairs the Service;
b) CenturyLink dispatches a technician to a Customer Site and the technician is unable to complete the work because Customer was not available when the technician arrived.
c) Customer incurs three false alarms in a month; in which case, Customer will pay a $300 false alarm fee, plus an additional fee for each additional false alarm during that month (except where CenturyLink provides the Internet connection). Customer may request that CenturyLink discontinue Service monitoring in order to avoid false alarm fees; provided, however, CenturyLink shall have no further monitoring obligations whatsoever with regard to the affected Service. CenturyLink may require the purchase of Incident Response ("IR") Services, which consist of CenturyLink personnel responding to security events impacting Customer. IR services are limited to response and mitigation of incidents and do not include ongoing or long-term security consulting, which are subject to additional terms and charges.

If a Service requires reconfiguration or retuning for any reason, including reducing false positives and nuisance alerts, CenturyLink will contact Customer, if necessary, to schedule the activity (typically during normal maintenance windows) and Customer agrees to cooperate with CenturyLink to schedule such activity. If CenturyLink determines that an emergency security change is required, CenturyLink will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

Definitions

An access control list (ACL): Is a list of permissions attached to a network device. The network device examines each packet to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access control list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

CenturyLink Service Center: The primary organization for resolving infrastructure issues that is staffed 24/7/365 to respond in a timely manner to incidents and requests pertaining to Customer IT infrastructure.

CenturyLink Managed Hosting Environment: CenturyLink provides hands-on installation within the Managed Hosting Environment.

Customer's Premises: CenturyLink ships device to Customer with installation instructions and telephone support. Customer installs equipment.

CenturyLink IDC Colocation Environment: CenturyLink provides hands-on installation within the CenturyLink IDC Colocation Environment.

Local Area Network (LAN): A local area network (LAN) is a computer network that interconnects computers within a limited area.

Maintenance Windows: A period of time designated in advance by CenturyLink, during which preventive maintenance that could cause disruption of service may be performed. Current Scheduled Maintenance windows are:

- Americas: Saturday 00:00AM to 5:00AM; Sunday 00:00AM to 5:00AM
- EMEA: Saturday 02:00AM to 6:00AM

- APAC (Except Japan): Saturday 21:00 (GMT) AM to Sunday 01(GMT)
- Japan: Sunday 04:00 (JST) to 8:00 (JST)

Managed Dedicated Network Intrusion Detection Service (NIDS): is a CenturyLink provided service that includes licensing, installation, configuration, administration, 24/7 monitoring, and maintenance and support of a CenturyLink-owned security device. The NIDS service includes access to secure web portal where IDS alerts are available for Customer review. CenturyLink Security Operations Center (SOC)